Marine Corps Intrusion Detection and Analysis Section (MIDAS)

Overview of Operations and Capabilities

2000

MIDAS MISSION

The MIDAS provides security centric network support at the Tactical, Operational and strategic levels to the operational war fighter as well as Posts, Bases and Stations that support the Marine Corps War Fighter

Mission Accomplished Through:

- Intrusion Detection
- Incident Handling
- Threat Analysis
- Virus Team
- Deployed Support
- Vulnerability Assessment

MIDAS Immediate Chain of Command

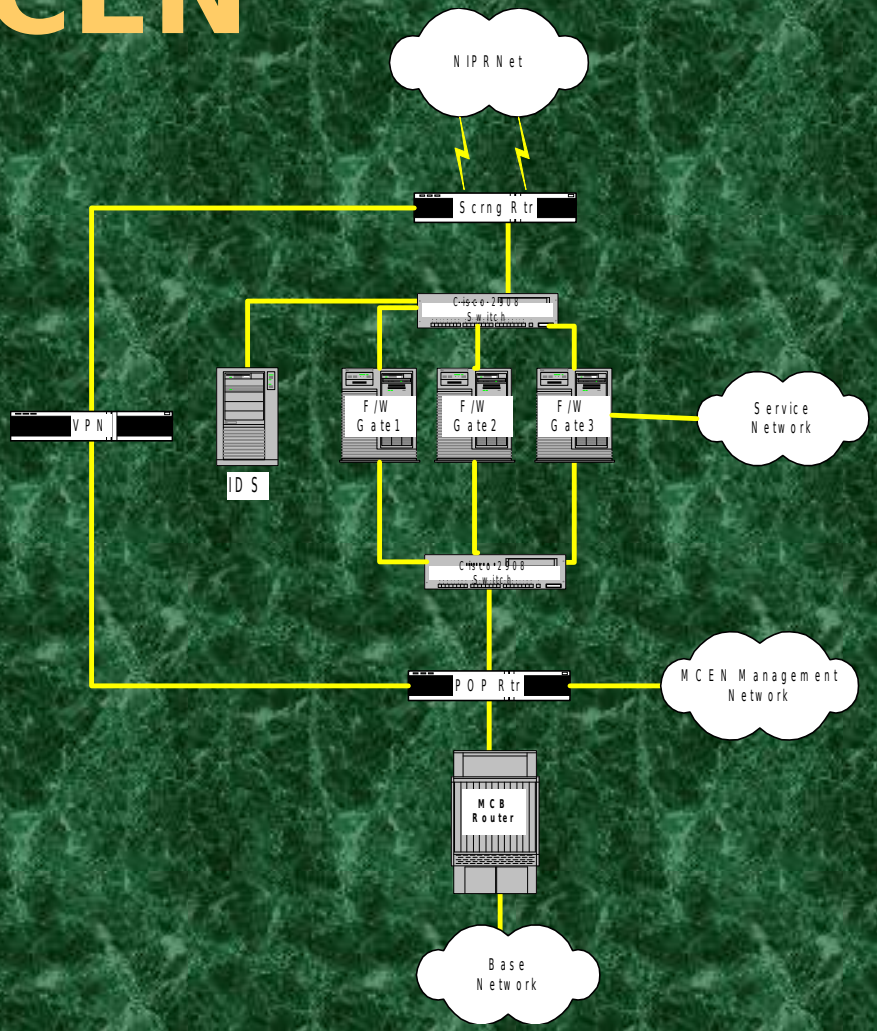
MIDAS OIC

- **Tactical Cell**
  - Deployed Security Interdiction Devices (DSID)
- **Operational Cell**
  - Garrison IDS Console and Detectors located throughout the MCEN
- **Strategic Cell**
  - MIDAS Threat Database (MTD) MIDAS Collection Database (MCD)

- MIDAS Web Page
- Forensic Analysis
- Virus Team

Topology of IDS in the MCEN

- Defense-in-Depth Strategy
- That which is not strictly permitted is denied
- IDS Technology



Tools Used to Aid CND

- Intrusion Detection System (RealSecure – COTS)
- Data Aggregation Tools
  - Routers
  - Firewalls
  - IDS
- MIDAS Collection Database (MCD)
- MIDAS Threat Database (MTD)

Intrusion Detection:

- Systems that collect information from a variety of systems and network resources, then analyze the information for signs of intrusion and misuse in near real-time.

Benefits of Intrusion Detection

- Improving the integrity of the information security infrastructure
- Improve system monitoring
- Tracing user activity from point of entry to point of exit or impact
- Recognizing and reporting alterations to data files

Benefits of Intrusion-Detection cont:

- Spotting errors of system configuration and sometimes correcting them
- Recognizing specific types of attacks and alerting appropriate staff for defensive responses
- keeping system management personnel up to date on recent corrections to programs

RealSecure Components

- **Detectors -**
  - Network Engine for network-based intrusion detection
  - System Agent for host-based intrusion detection
- **Management Console** – Provides:
  - Central Real-time alarm management
  - Central data management
  - Central detector configuration

Management Console

- Collects databases from active detectors into a single data store:
  - For export to an enterprise database system
  - To generate reports

Network Detectors

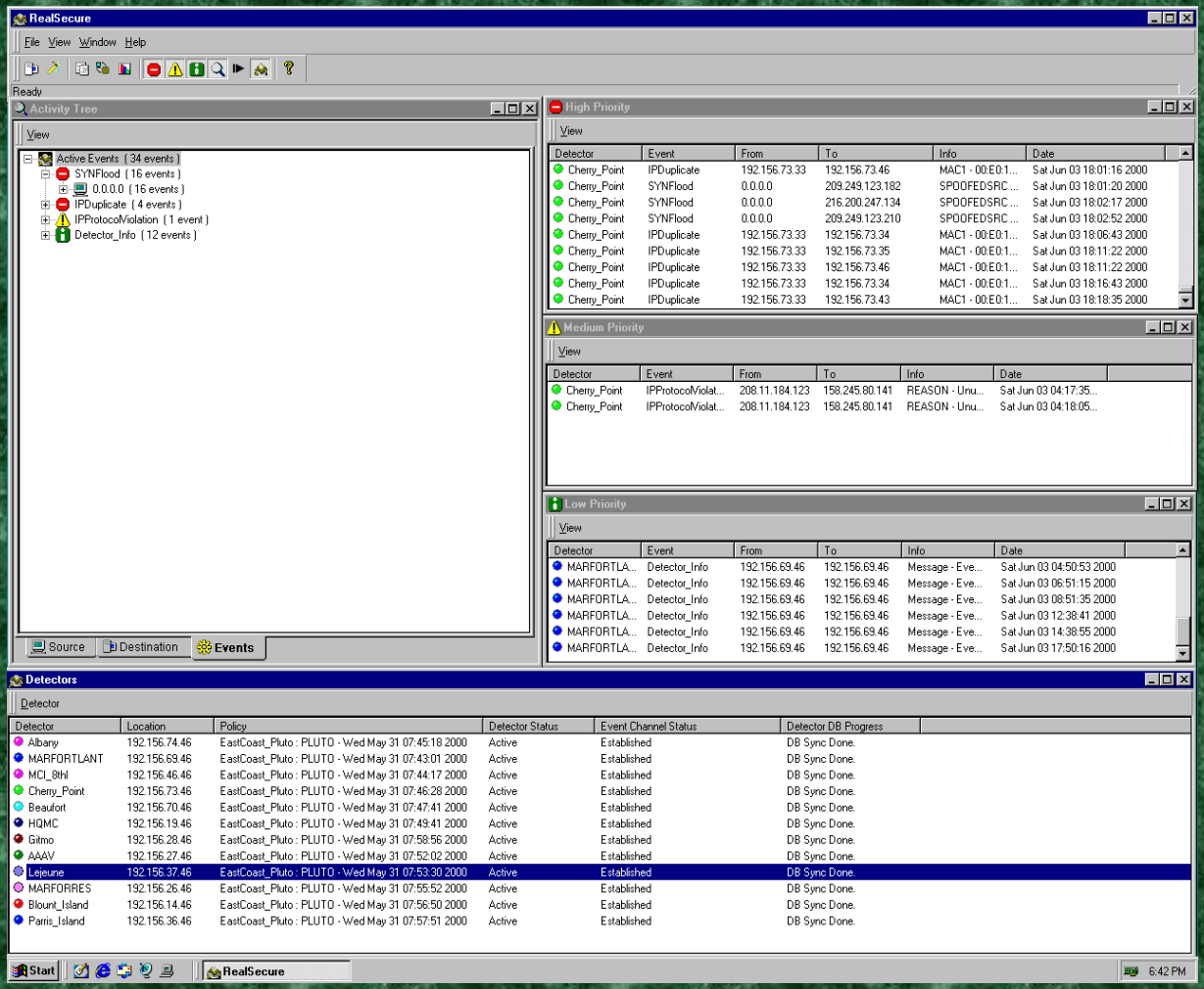
- Captures all packets from a local network segment
- Examines each packet for signs of:
  - Network abuse
  - Malicious intent
  - Suspicious activity

Network Detectors cont.

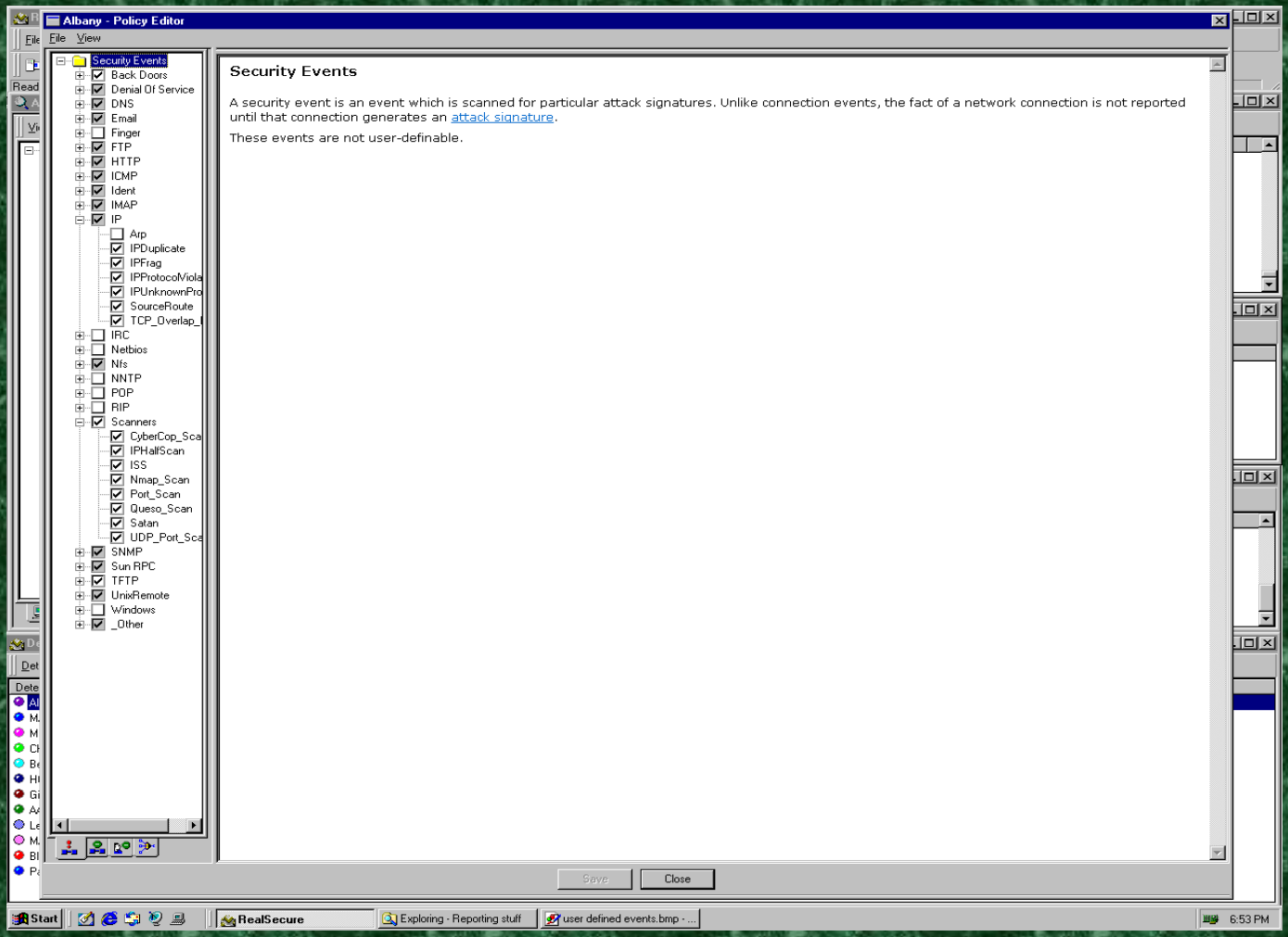
- Users can customize by:
  - Defining connection events
  - Specifying a response for every single event
  - Fine-tuning existing signatures
  - Establish traffic masking filters

RealSecure Demo

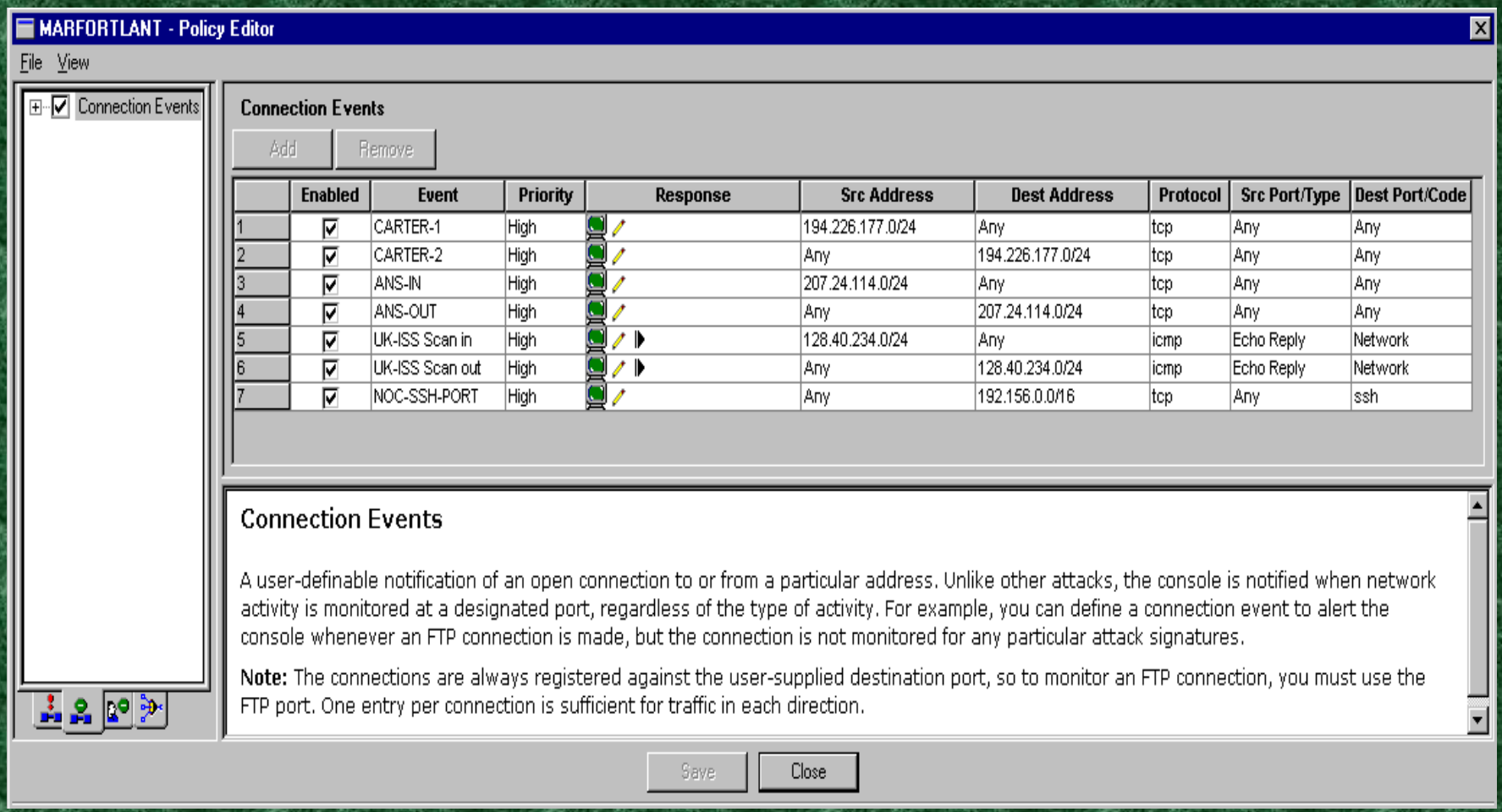
Console Main Screen



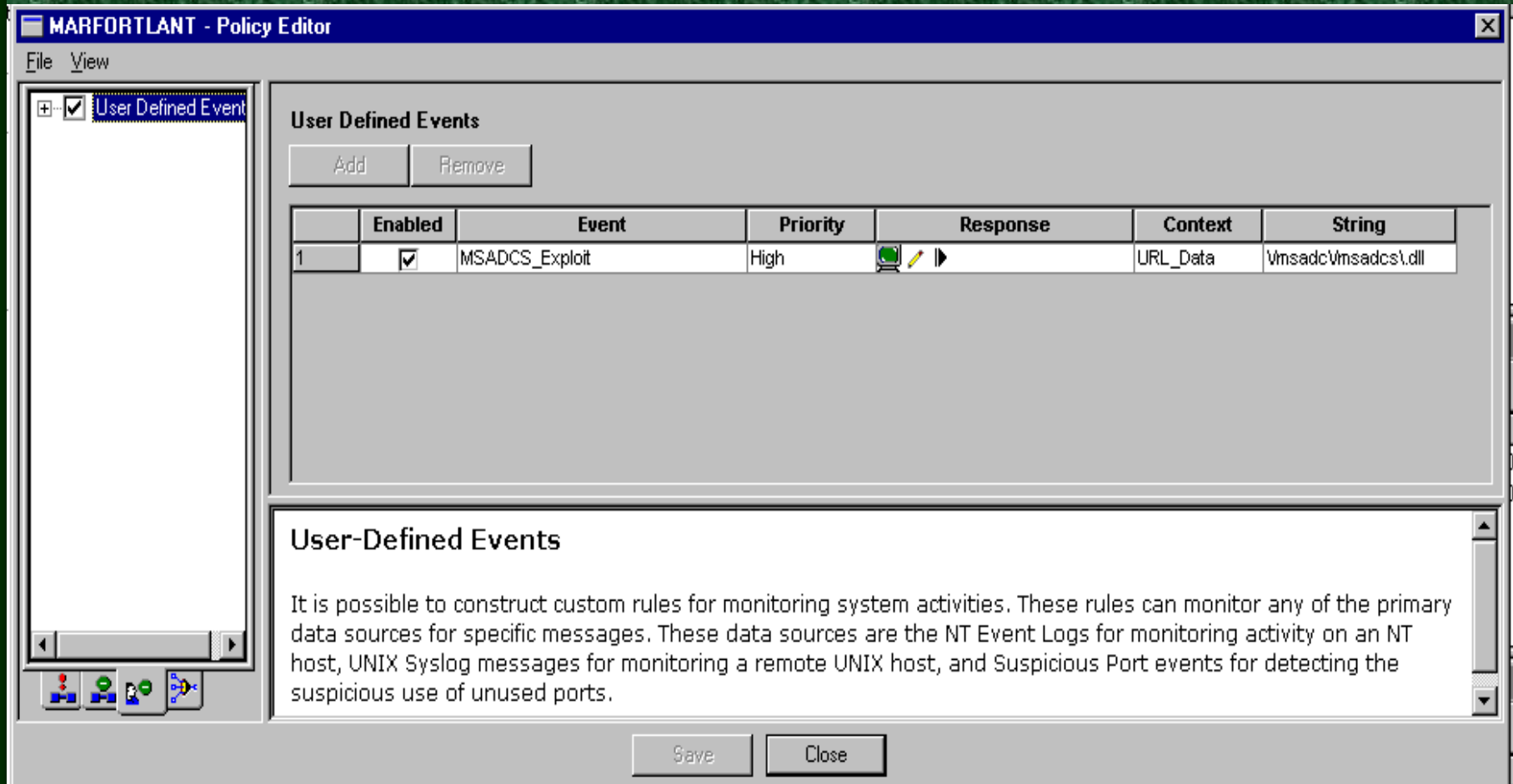
Policy Editor



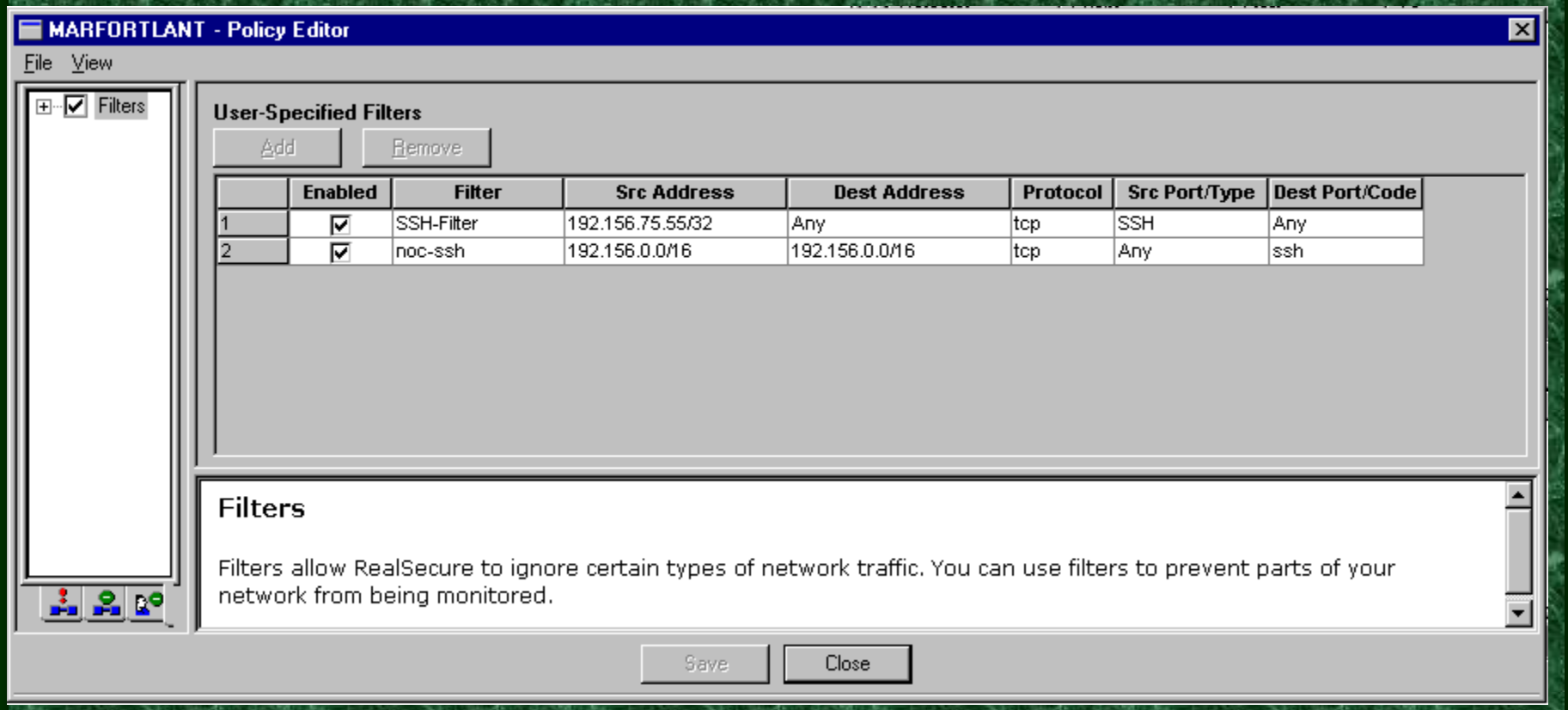
Connection Events



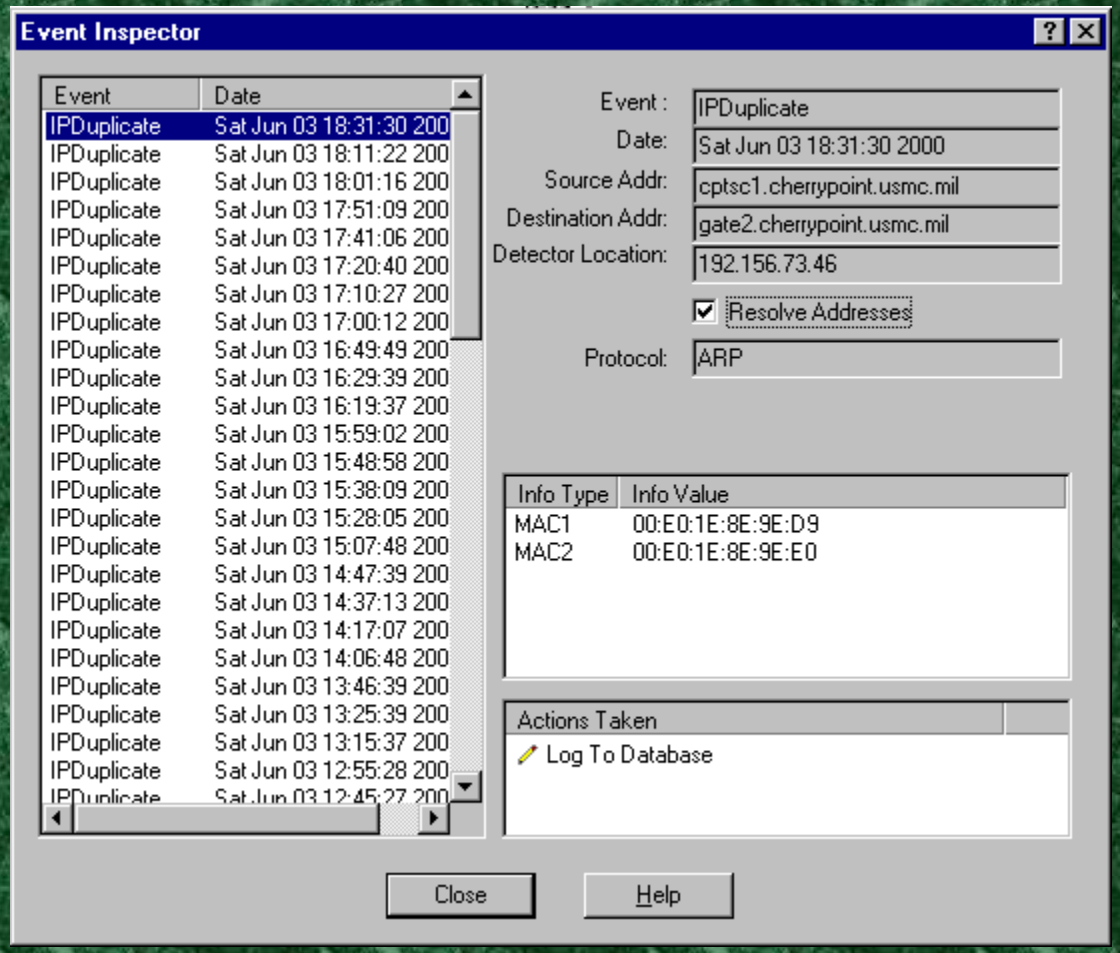
User Defined Events



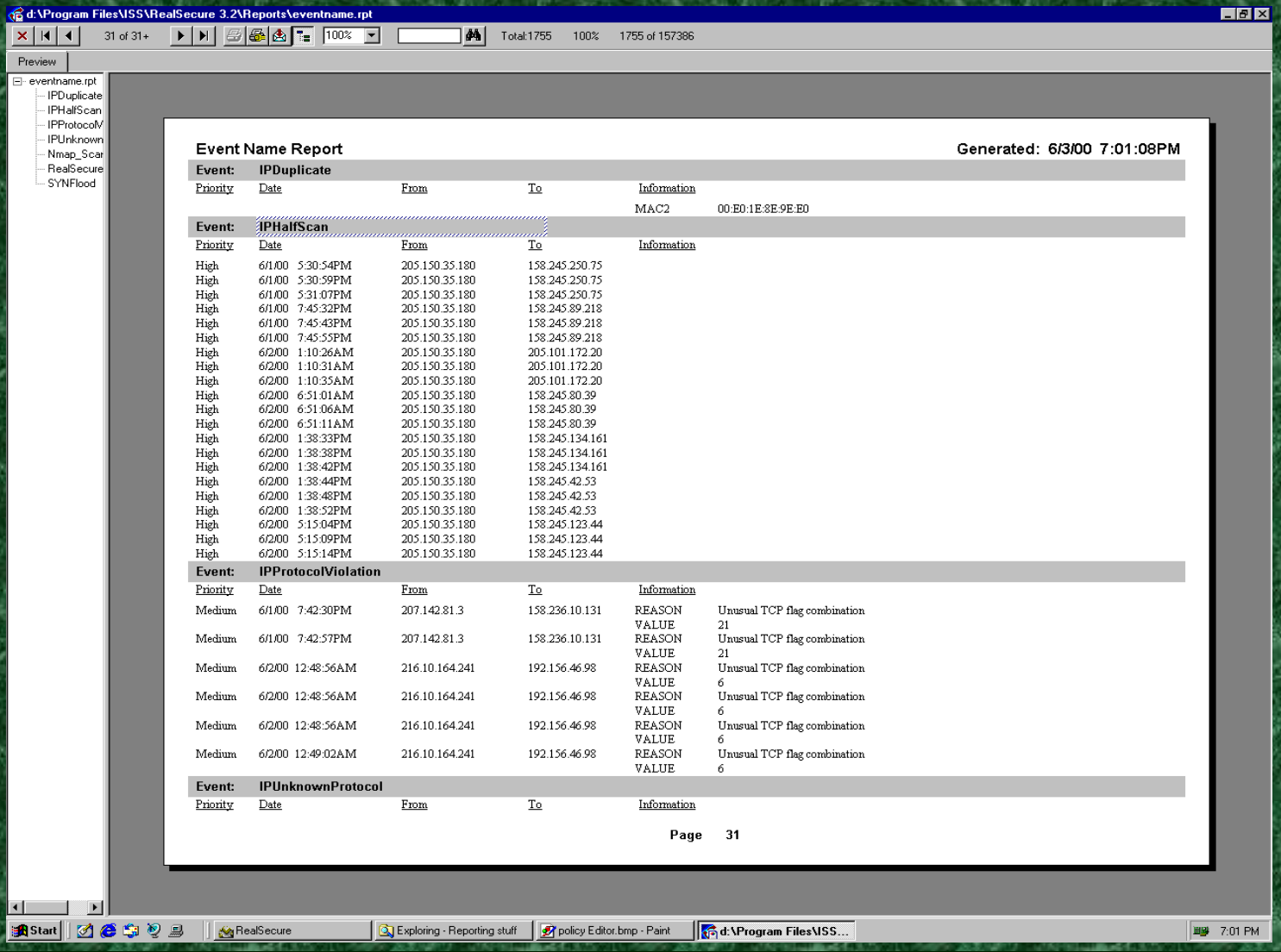
Filters


MARFORTLANT - Policy Editor
File View
Filters
User-Specified Filters
Add
Remove
Enabled
Filter
Src Address
Dest Address
Protocol
Src Port/Type
Dest Port/Code
1
SSH-Filter
192.156.75.55/32
Any
tcp
SSH
Any
2
noc-ssh
192.156.0.0/16
192.156.0.0/16
tcp
Any
ssh
Filters
Filters allow RealSecure to ignore certain types of network traffic. You can use filters to prevent parts of your network from being monitored.
Save
Close

Event Inspector



Event Name Report



Event Name Report — **Generated: 6/3/00 7:01:08PM**

Event: IPDuplicate

Priority	Date	From	To	Information	
				MAC2	00:E0:1E:8E:9E:E0

Event: IPHalfScan

Priority	Date	From	To	Information
High	6/1/00 5:30:54PM	205.150.35.180	158.245.250.75	
High	6/1/00 5:30:59PM	205.150.35.180	158.245.250.75	
High	6/1/00 5:31:07PM	205.150.35.180	158.245.250.75	
High	6/1/00 7:45:32PM	205.150.35.180	158.245.89.218	
High	6/1/00 7:45:43PM	205.150.35.180	158.245.89.218	
High	6/1/00 7:45:55PM	205.150.35.180	158.245.89.218	
High	6/2/00 1:10:26AM	205.150.35.180	205.101.172.20	
High	6/2/00 1:10:31AM	205.150.35.180	205.101.172.20	
High	6/2/00 1:10:35AM	205.150.35.180	205.101.172.20	
High	6/2/00 6:51:01AM	205.150.35.180	158.245.80.39	
High	6/2/00 6:51:06AM	205.150.35.180	158.245.80.39	
High	6/2/00 6:51:11AM	205.150.35.180	158.245.80.39	
High	6/2/00 1:38:33PM	205.150.35.180	158.245.134.161	
High	6/2/00 1:38:38PM	205.150.35.180	158.245.134.161	
High	6/2/00 1:38:42PM	205.150.35.180	158.245.134.161	
High	6/2/00 1:38:44PM	205.150.35.180	158.245.42.53	
High	6/2/00 1:38:48PM	205.150.35.180	158.245.42.53	
High	6/2/00 1:38:52PM	205.150.35.180	158.245.42.53	
High	6/2/00 5:15:04PM	205.150.35.180	158.245.123.44	
High	6/2/00 5:15:09PM	205.150.35.180	158.245.123.44	
High	6/2/00 5:15:14PM	205.150.35.180	158.245.123.44	

Event: IPProtocolViolation

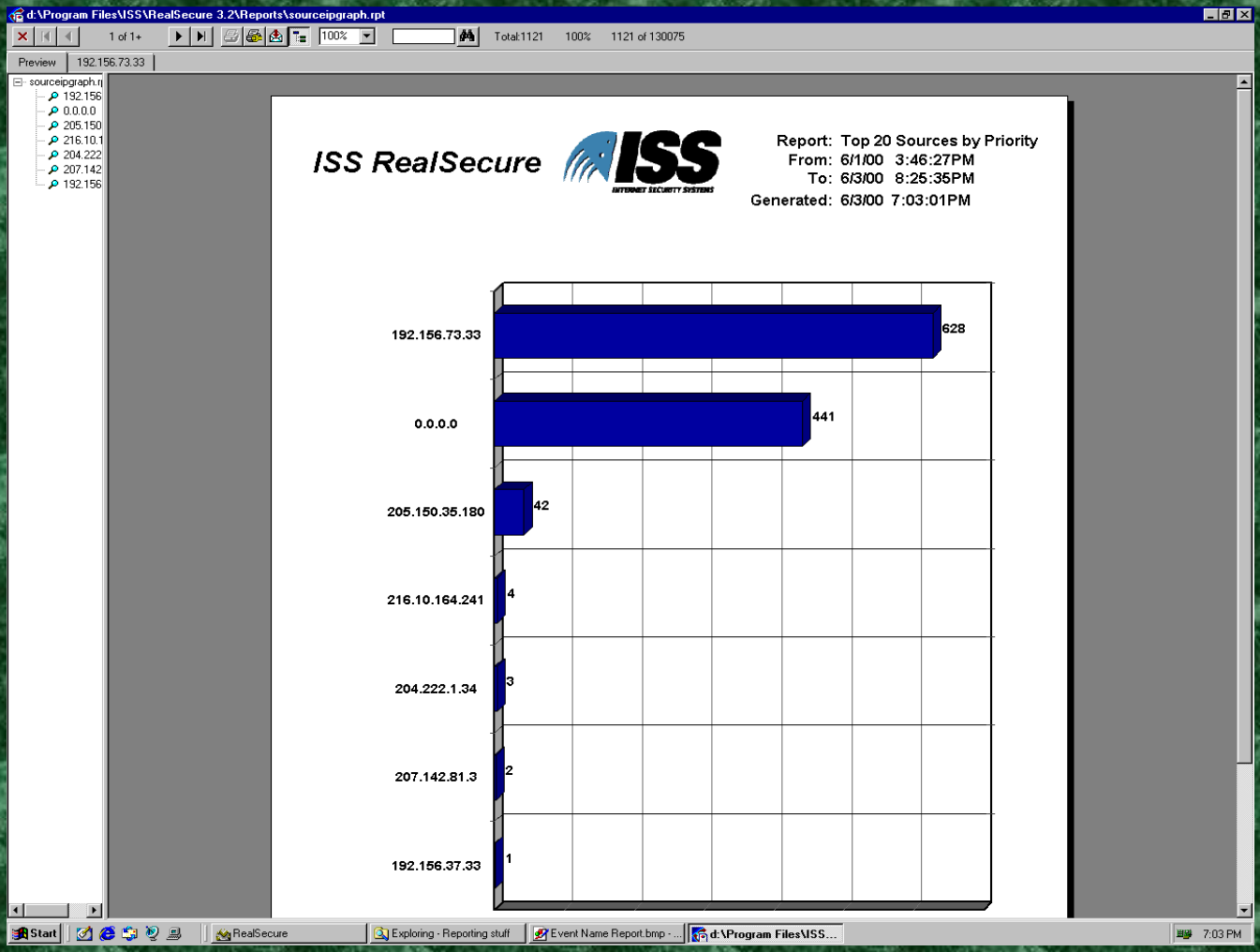
Priority	Date	From	To	Information	
Medium	6/1/00 7:42:30PM	207.142.81.3	158.236.10.131	REASON VALUE	Unusual TCP flag combination 21
Medium	6/1/00 7:42:57PM	207.142.81.3	158.236.10.131	REASON VALUE	Unusual TCP flag combination 21
Medium	6/2/00 12:48:56AM	216.10.164.241	192.156.46.98	REASON VALUE	Unusual TCP flag combination 6
Medium	6/2/00 12:48:56AM	216.10.164.241	192.156.46.98	REASON VALUE	Unusual TCP flag combination 6
Medium	6/2/00 12:48:56AM	216.10.164.241	192.156.46.98	REASON VALUE	Unusual TCP flag combination 6
Medium	6/2/00 12:49:02AM	216.10.164.241	192.156.46.98	REASON VALUE	Unusual TCP flag combination 6

Event: IPUnknownProtocol

Priority	Date	From	To	Information

Page 31

Graph


d:\Program Files\ISS\RealSecure 3.2\Reports\sourceipgraph.rpt
Total:1121
100%
1121 of 130075
Preview
192.156.73.33
ISS RealSecure
Report: Top 20 Sources by Priority
From: 6/1/00 3:46:27PM
To: 6/3/00 8:25:35PM
Generated: 6/3/00 7:03:01PM
192.156.73.33
628
0.0.0.0
441
205.150.35.180
42
216.10.164.241
4
204.222.1.34
3
207.142.81.3
2
192.156.37.33
1
Start
RealSecure
Exploring - Reporting stuff
Event Name Report.bmp - ...
d:\Program Files\ISS...
7:03 PM

Raw Logs (RealSecure)

Microsoft Access - [RSLog : Table]

File Edit View Insert Format Records Tools Window Help

ID	EventDate	EventName	ProtocolID	SourcePort	DestinationPor	SourcePortNar	DestinationPor	SourceAddres	DestinationAdd	S
2616888	30 12:48:35 AM	SYNFlood	6	0	80	Any	HTTP	0	1759267281	0
2616889	/00 1:13:39 AM	SYNFlood	6	0	80	Any	HTTP	0	-2111048567	0
2616890	/00 1:21:45 AM	SYNFlood	6	0	80	Any	HTTP	0	-1395853616	0
2616891	/00 1:23:22 AM	IPHalfScan	6	64	1521	64	1521	667485708	1928457374	1
2616892	/00 2:58:20 AM	SYNFlood	6	0	25	Any	E-mail	0	603118018	0
2616893	/00 3:31:00 AM	SYNFlood	6	0	25	Any	E-mail	0	586340802	0
2616894	/00 3:33:30 AM	SYNFlood	6	0	25	Any	E-mail	0	250796482	0
2616895	/00 3:34:45 AM	SYNFlood	6	0	25	Any	E-mail	0	116578754	0
2616896	/00 3:56:53 AM	SYNFlood	6	0	1601	Any	1601	0	40660429	0
2616897	/00 4:55:10 AM	SYNFlood	6	0	80	Any	HTTP	0	682160333	0
2616898	/00 5:47:29 AM	SYNFlood	6	0	80	Any	HTTP	0	-126934824	0
2616899	/00 6:49:52 AM	SYNFlood	6	0	80	Any	HTTP	0	438995663	0
2616900	/00 7:20:51 AM	SYNFlood	6	0	8080	Any	Httpd	0	-101401395	0
2616901	/00 7:44:29 AM	SYNFlood	6	0	80	Any	HTTP	0	1556029656	0
2616902	/00 7:53:46 AM	SYNFlood	6	0	80	Any	HTTP	0	-1272680744	0
2616903	/00 8:34:27 AM	SYNFlood	6	0	80	Any	HTTP	0	232784337	0
2616904	/00 8:39:44 AM	SYNFlood	6	0	25	Any	E-mail	0	50364360	0
2637923	/00 8:56:33 AM	SYNFlood	6	0	80	Any	HTTP	0	216007121	0
2637924	/00 9:03:04 AM	SYNFlood	6	0	80	Any	HTTP	0	199229905	0
2637925	/00 9:04:39 AM	SYNFlood	6	0	80	Any	HTTP	0	316670417	0
2637926	/00 9:05:02 AM	SYNFlood	6	0	80	Any	HTTP	0	299893201	0
2637927	/00 9:05:02 AM	SYNFlood	6	0	80	Any	HTTP	0	266338769	0
2637928	/00 9:05:10 AM	SYNFlood	6	0	80	Any	HTTP	0	249561553	0
2637929	/00 9:05:42 AM	SYNFlood	6	0	80	Any	HTTP	0	283115985	0
2637930	/00 9:38:26 AM	SYNFlood	6	0	80	Any	HTTP	0	1556029656	0
2637931	30 11:33:07 AM	SYNFlood	6	0	80	Any	HTTP	0	-141908019	0
2637932	30 12:28:51 PM	SYNFlood	6	0	80	Any	HTTP	0	-2011160104	0
2637933	30 12:53:09 PM	SYNFlood	6	0	80	Any	HTTP	0	232784337	0
2637934	/00 1:04:20 PM	SYNFlood	6	0	443	Any	HTTPS	0	133374168	0
2637935	/00 1:21:11 PM	SYNFlood	6	0	80	Any	HTTP	0	-1912370483	0
2637936	/00 1:21:15 PM	SYNFlood	6	0	80	Any	HTTP	0	-2014070319	0
2637937	/00 1:22:19 PM	SYNFlood	6	0	80	Any	HTTP	0	704875213	0
2637938	/00 1:23:14 PM	SYNFlood	6	0	80	Any	HTTP	0	1711508173	0
2637939	/00 1:23:36 PM	SYNFlood	6	0	80	Any	HTTP	0	-1241281843	0
2637940	/00 1:26:30 PM	SYNFlood	6	0	80	Any	HTTP	0	369330893	0
2637941	/00 1:27:45 PM	SYNFlood	6	0	80	Any	HTTP	0	1375963863	0

Record: 9 of 128968

0=TCP,1=UDP,2=ICMP, 3=Unknown or ARP.

NUM

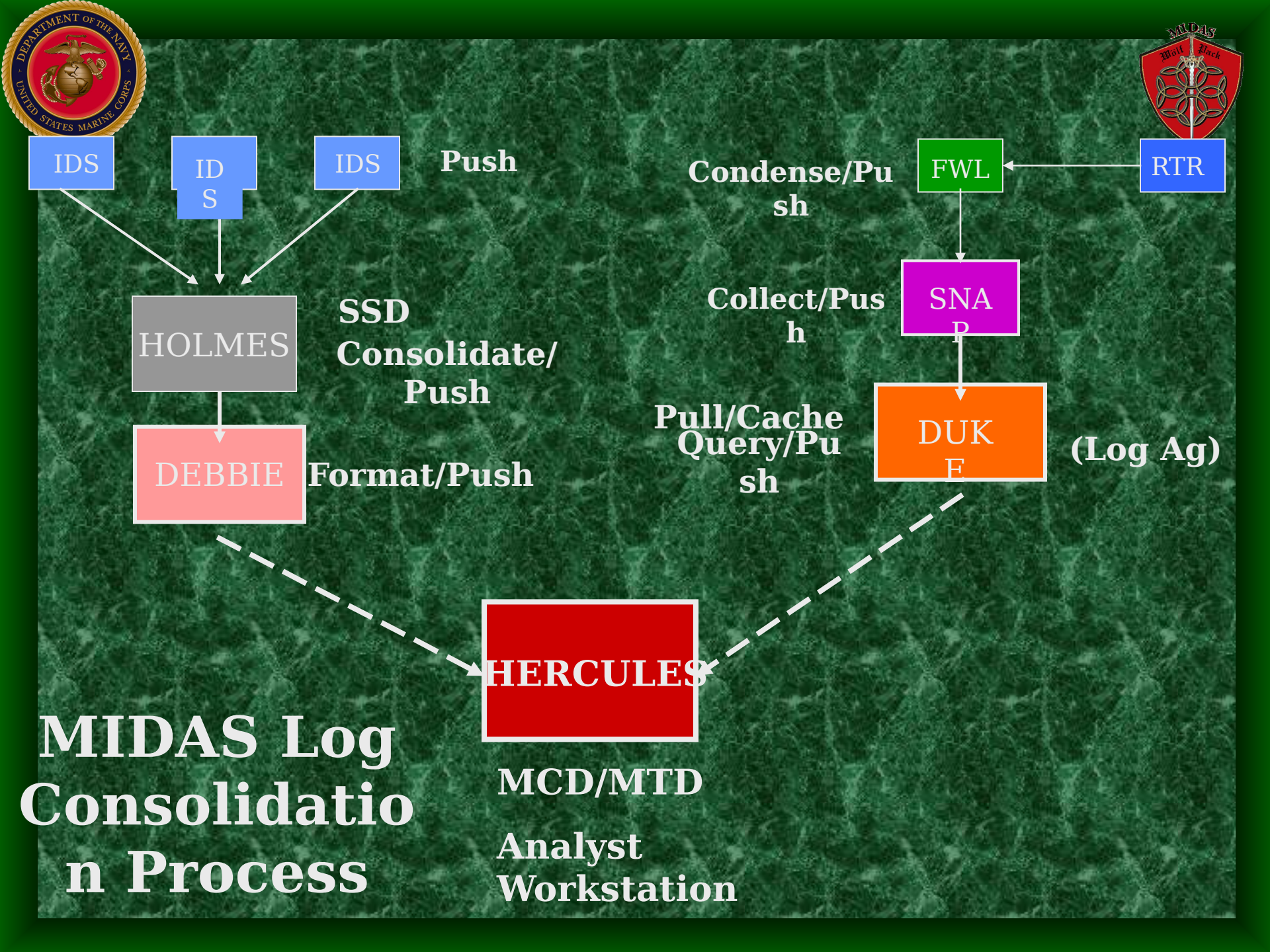
Data Collection and Reporting

Log file Aggregation

JCD - MCD – MTD

Log File Aggregation Tool

- Capabilities
  - Ability to aggregate Firewall, Router and IDS logs
  - Central repository
  - Ability to query on one or more data sets


IDS
IDS
IDS
Push
HOLMES
SSD
Consolidate/
Push
DEBBIE
Format/Push
Condense/Pu
sh
FWL
RTR
Collect/Pus
h
SNA
P
Pull/Cache
Query/Pu
sh
DUK
E
(Log Ag)
HERCULES
MCD/MTD
Analyst
Workstation
MIDAS Log
Consolidatio
n Process

Joint Cert Database (JCD)

- Needed common database for all to use.
- Managed by JTF-CND
- Operated by DOD-CERT (Technical Arm of JTF-CND)

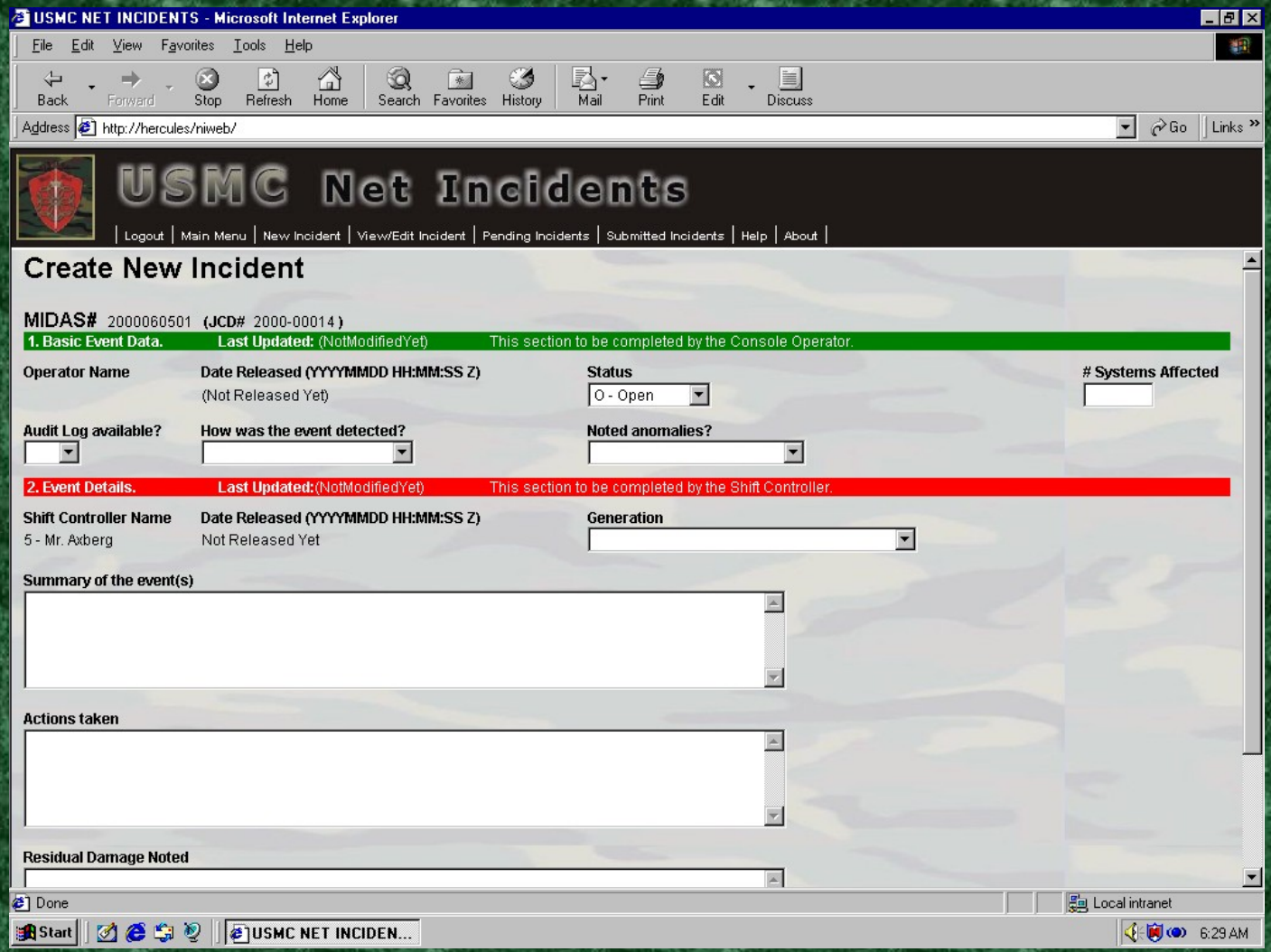
MIDAS Collection Database (MCD)

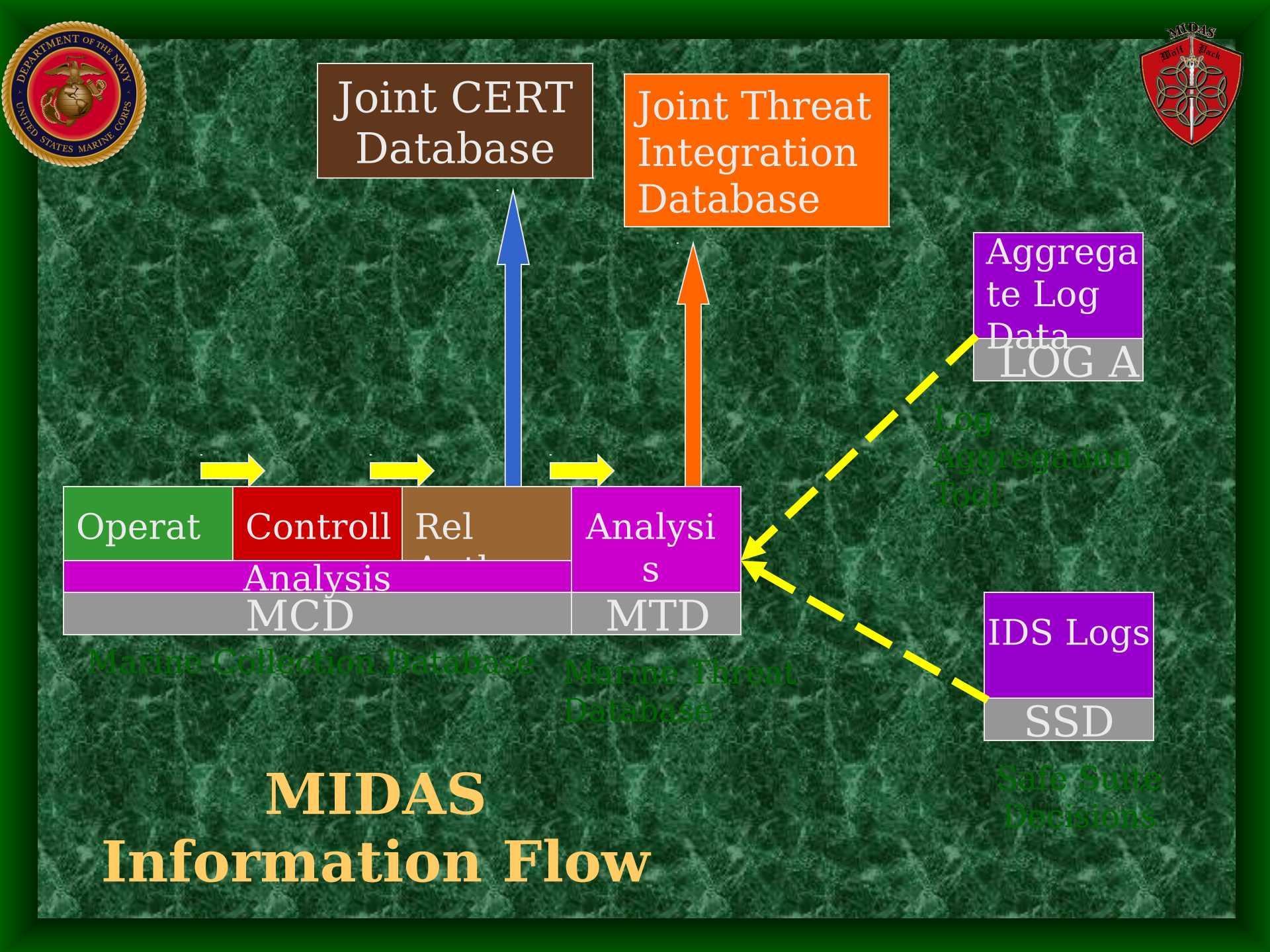
- Purpose
  - Maintain a coherent MCEN specific event / incident database
  - Vehicle for reporting MCEN incidents to the DOD-CERT via the Joint CERT Database (JCD)

MCD Capabilities

- Provides 3 levels of authority
  - Console Operator
  - Shift Controller
  - Releasing Authority
- Holds responsible parties to task
- Eliminates over-redundancy
- Easily accessible for viewing

View of MCD Interface




Joint CERT Database
Joint Threat Integration Database
Aggrega te Log Data
LOG A
Log Aggregation Tool
Operat
Controll
Rel
Analysi s
Analysis
MCD
MTD
Marine Collection Database
Marine Threat Database
IDS Logs
SSD
Safe Suite Decisions
MIDAS
Information Flow

STRATEGIC ANALYSIS

- Analyze All MCEN logs archived
- Key on trends
- Build Profiles
- Prepare and disseminate time-sensitive

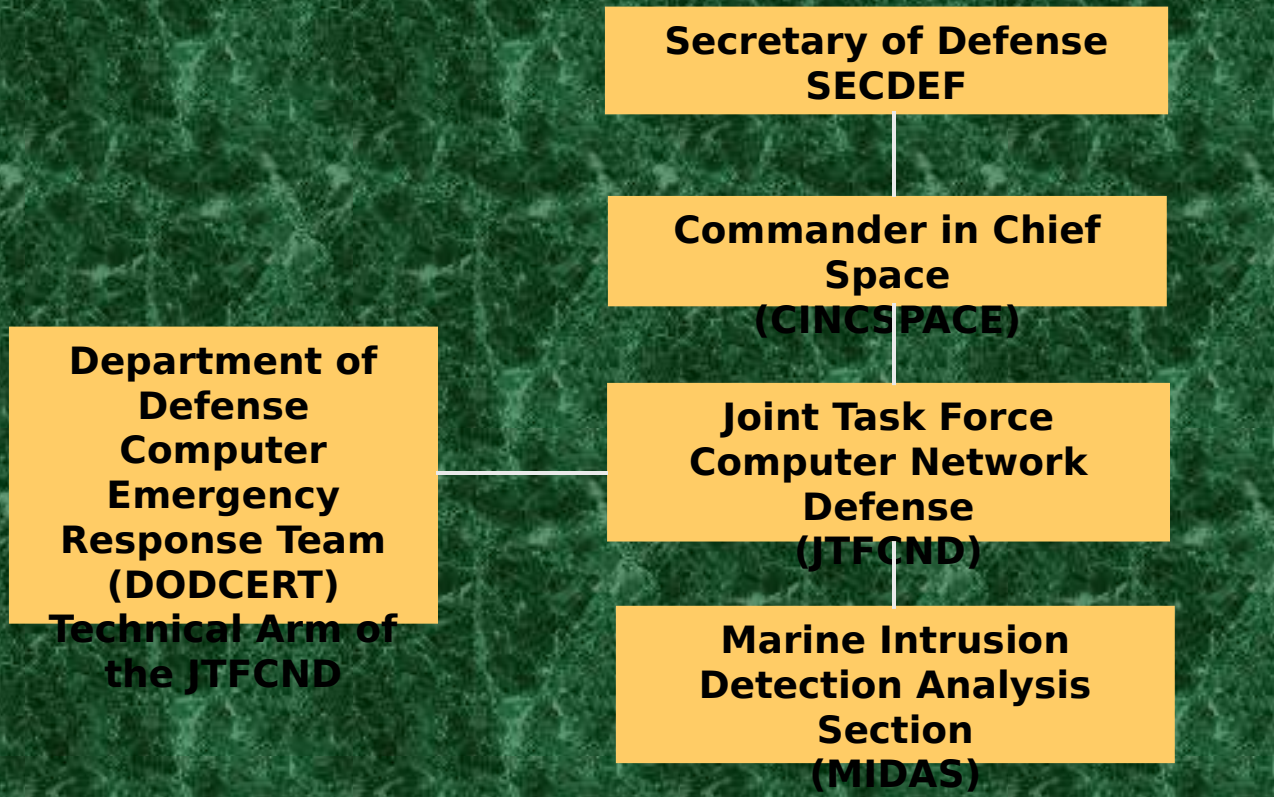
Evaluations of the scope and immediacy o
Cyber Threats posed by individuals and
Groups in the U.S. and abroad.

- Manage the Marine Threat Database (MT

MTD Capabilities

- Maintain profiles on hostile entities
  - Nation States
  - Terrorist cells/groups
  - Hacker(s) and hacker groups
  - Other entities having malicious intent
- Maintain historical data from multiple sources relevant to ongoing analysis
- Ability to infuse immediate threat analysis in order to effect current and future incidents

Incident Reporting Chain of Command



QUESTIONS ?